The nature of trust in the online world

By Peter Grabosky

Originally published: The Age, 23 April 2001, I.T.1, pp. 1,12

Ever since human beings began to claim ownership over property, other human beings have sought to take it from them. In the past quarter of a century, with the arrival of digital technology, both property and theft have taken on new forms.

Money, music, text and video are now commonly stored and transferred electronically in the form of a long series of zeroes and ones. And they can be stolen with a laptop computer from one's bedroom.

The growth in connectivity of computing and communications, and their applications to electronic commerce, increase both the number of prospective victims of computer-related crime and the number of prospective offenders.

As the Internet becomes increasingly a medium of commerce, it will also become increasingly a medium of fraud. Many traditional frauds, such as pyramid schemes and endless variations on advance-fee scams, lend themselves easily to the digital environment. So too does the non-delivery of products, or the delivery of defective merchandise.

Creative criminals are now able to use digital technology to do what criminals have always done, and more. Many types of electronic theft are essentially traditional forms of theft in new guises. It is the means of committing the theft - the fact that the criminal act can occur at the speed of light, and the fact that a thief can commit the act from the other side of the world - that are without precedent.

As recently as 1990, few people could even envisage what has since come to be known as the World Wide Web, and the possibility that an ordinary individual could communicate with millions of others seemed remote. Such communication can be for legitimate purposes, or otherwise. Cyberspace now abounds with a wide variety of investment opportunities, some of them legitimate, others bodgy. The introduction of the Internet has been accompanied by unprecedented opportunities for misinformation, and fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at negligible cost.

Ordinary investors are now able to buy and sell shares online without dealing through intermediaries such as underwriters, brokers and investment advisers. While this may enhance the efficiency of securities markets, it also provides opportunities for criminal exploitation. But the fundamental criminality of online securities fraud is still reducible to the basics: misrepresenting the underlying value of a security at the time of the initial public offering; or market manipulation during secondary trading of a security, through the dissemination of false information; or by engineering a deceptive pattern of transactions to attract the attention of the unwitting investor.

As government services are increasingly provided through online facilities, and payments to governments increasingly made electronically, so will the opportunities for fraud increase. Government benefit systems such as social security and health insurance are increasingly the subject of manipulation by individuals seeking to obtain more than their legal entitlement.

Salary systems may be similarly attractive as targets, and, in the case of taxation systems, including customs and excise fraud, some people will seek to evade payment either in part or altogether.

New technologies can also assist the crime of extortion in a variety of ways. The Internet can be used to communicate an extortion threat. A financial institution or other organisation's information systems may be specified as the target of a threat. In cases of blackmail, the Internet can be used to communicate embarrassing or harmful information. When an extortion entails some financial consideration, electronic payment systems may be used to transfer the funds.

And, finally, the Internet and World Wide Web may be incidental to the offence in question, such as when they are used to gather information about a prospective victim.

Originally, the law of theft applied only to something that could be physically removed and the law of fraud only to deception of another person in order to obtain something of value. But today, most developed countries make it an offence to steal telephone or Internet services, transfer funds electronically without permission from someone else's bank account into yours or to defraud an automatic teller machine.

In some areas, though, the law has not kept up with technology.

Most prominent among these are the commercial acquisition of personal information and various activities relating to digital piracy.

Today, in our "wired society", consumers leave many tracks. Data-matching technologies now permit the merging of otherwise disparate personal information in a manner that allows the collection and concentration of considerable detail about an individual. These details can include spending patterns and consumer preferences, photographic images, electronic correspondence and even the websites that one visits. Where health records are maintained on databases, it may be possible to ascertain an individual's entire medical history.

This information may have substantial commercial value but the collection and dissemination of such information can occur without the subject's knowledge or consent.

This can facilitate customer service in the new world of e-commerce, but misuse of this information for purposes of stalking, harassment, intimidation or commercial manipulation is common. As is the case with many computer-related mishaps, a great deal of private information can also be disclosed by accident.

Data on thousands of patients of the University of Michigan health system were inadvertently made available on the Internet for a period of at least two months, until a student discovered the error by chance in February 1999. The lapse occurred when the hospital was developing a new patient-scheduling system. The company installing the system had been given access to what was thought to be a secure server.

This raises questions about just what kind of personal details are in the public domain and whether publicly available data can become transformed into private personal information. One might also ask: Who owns it? In some parts of the world, Internet service providers have been known to buy or sell subscribers' personal information. In 1999, the attorney-general of Minnesota alleged that a bank sold the private financial details of customers to a telemarketing company for $US4 million plus commissions. The details were extensive and were reported to have included telephone and social security numbers, marital status, home-ownership, bankruptcy status, credit-card details, bank account balances and information on recent transactions.

Whether and how the electronic data mining of personal information should be regarded as misappropriation, how it should be regulated and in what circumstances it should be made illegal are issues that confront policymakers today.

Of course, the digital age is not the first time new technologies have influenced the development of law. Copyright law has an interesting origin, sprouting from efforts to control sedition after the invention of the printing press. But intellectual property has been the subject of a great deal of legal manoeuvring in recent years, as digital technology permits the instantaneous and almost perfect reproduction of text, sound, images and multimedia.

As the entertainment and software industries, among others, remind us, uncontrolled piracy worldwide costs billions of dollars, can remove the incentive for creative work and can chill the development and expansion of entire industries. And it is not just Bill Gates who suffers. One aspiring Chinese rock band recently released two CDs, each of which was pirated and published free on the Internet before they were available for legitimate purchase.

Rampant piracy can stifle the growth of information technology and the economic development on which it is based. To the extent that budding IT entrepreneurs in developing countries are thwarted by the lack of protection for their intellectual property, entire economies can suffer.

Consider Vietnam, where it is estimated that more than 95 per cent of software in use has been pirated. What incentives exist for a young computer programmer to develop truly innovative products?

Globalisation itself brings difficulties for enforcement of copyright, since distribution of works crosses international boundaries and may occur simultaneously in several distinct jurisdictions.

The problem of piracy is compounded by the limited law enforcement resources of governments in most countries where laws against piracy do exist. With crimes like illicit drug trafficking, illegal immigration and fraud against governments themselves high on the enforcement agenda, the pursuit of electronic pirates takes on a lower priority. This places considerable burdens upon the victim, whose first line of defence is often self-help.

In some circumstances, civil remedies such as compensatory damages and injunctions to restrain objectionable conduct may provide effective relief, but, in others, an individual or company whose work has been pirated may have little recourse.

A potentially more promising solution lies in technological developments that can provide a modicum of protection against information piracy. This can include encrypting data so it is accessible only to authorised persons or including technologies that detect and disclose unauthorised reproductions.

For example, consider a digital equivalent of tamper-proof packaging. The copyright owner can put hidden cues in the data so that if people make inappropriate use of it, such misuse becomes boldly evident.

So-called "digital watermarking" can ensure a trail of evidence if unauthorised copying does occur. Watermarks can be perceptible to the naked eye, imperceptible, or a combination of both. They may also contain information that allows other programs, sometimes called "bots", to track them where the copy appears on a Web page.

Inbuilt security software embedded in a CD or in text can also be used to direct the data to effectively degrade itself or self-destruct if stipulated conditions are not met. This is similar to the use of dye-packs in banknotes as a countermeasure against robbery.

The development of technologies to combat piracy will remain one of the growth areas of the information age.

The challenge of combating electronic theft is one we all face. Just as we cannot depend upon police patrols to prevent household burglary or motor vehicle theft (there are just not enough police to go around), we cannot depend upon "cyber cops" to protect our digital assets. There are relatively few skilled computer crime investigators and forensic accountants in our police services and they usually have more work than they can handle.

The rarity of suitably trained investigators generates competition for scarce investigative resources. This forces a choice between concentrating efforts on protecting property interests or focusing on areas that have attracted greater concern from the public.

Trust is the foundation of commerce in cyberspace, just as it is on the ground. The difference is that, in real life, trust is based on personal relationships, while online trust is based on confidence in processes. The establishment of trusted processes in cyberspace is the key to commercial success. So it is that online merchants seek to create an environment in which a prospective customer can be relaxed and confident about any prospective transactions.

The establishment of trust will depend upon technology no less than it will depend on law.

We depend on markets to deliver solutions where governments cannot. As and where markets succeed, ours will be a world in which honest individuals and organisations will be better equipped to protect themselves.

Dr Peter Grabosky is Deputy Director and Director of Research at the Australian Institute of Criminology in Canberra. He is co-author, with Dr Russell G. Smith and Dr Gillian Dempsey, of *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press 2001).